

2016 Emerging Technology Domains Risk Survey

Christopher King
Dan Klinedinst
Todd Lewellen
Garret Wassermann

April 2016

TECHNICAL REPORT
CMU/SEI-2016-TR-003

CERT® Coordination Center

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

<http://www.sei.cmu.edu>



Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0003445

Table of Contents

Executive Summary	v
Abstract	vii
1 Introduction	1
2 Methodology	3
3 Augmented Reality	8
3.1 Introduction	8
3.2 Recommendation	8
3.3 Time Frame	8
3.4 Risks	8
3.5 Exploitation Examples	8
4 Connected Home	10
4.1 Introduction	10
4.2 Recommendation	10
4.3 Time Frame	10
4.4 Risks	10
4.5 Exploitation Examples	10
5 Enterprise 3D Printing (Additive Manufacturing)	11
5.1 Introduction	11
5.2 Recommendation	11
5.3 Time Frame	11
5.4 Risks	11
5.5 Likelihood of Domain Success	12
5.6 Exploitation Examples	12
6 Networked Telematics	13
6.1 Introduction	13
6.2 Recommendation	13
6.3 Time Frame	13
6.4 Risks	13
6.5 Likelihood of Domain Success	13
6.6 Exploitation Examples	13
7 Smart Medical Devices	15
7.1 Introduction	15
7.2 Recommendation	15
7.3 Time Frame	15
7.4 Risks	15
7.5 Likelihood of Domain Success	15
7.6 Exploitation Examples	15
8 Autonomous Machines	16
8.1 Introduction	16
8.2 Recommendation	16
8.3 Time Frame	16
8.4 Impact	16
8.5 Exploitation Examples	16

9	Smart Sensors	17
9.1	Introduction	17
9.2	Recommendation	17
9.3	Time Frame	17
9.4	Risks	17
9.5	Likelihood of Domain Success	18
9.6	Exploitation Examples	18
10	Commercial Unmanned Aerial Vehicles	19
10.1	Introduction	19
10.2	Recommendation	19
10.3	Time Frame	19
10.4	Risks	19
10.5	Likelihood of Domain Success	19
10.6	Exploitation Examples	19
11	Vehicle Autonomy (Driverless Cars)	21
11.1	Introduction	21
11.2	Recommendation	22
11.3	Time Frame	22
11.4	Risks	22
11.5	Likelihood of Domain Success	23
11.6	Exploitation Examples	23
12	Vehicular Communication Systems	24
12.1	Introduction	24
12.2	Recommendation	24
12.3	Time Frame	24
12.4	Risks	24
12.5	Likelihood of Domain Success	24
12.6	Exploitation Examples	25
13	Conclusion	26
	Appendix A: Underlying Technologies	27
	References/Bibliography	31

List of Figures

Figure 1: Communication Layers, Standards, and Technologies [Tele-Worx 2014]	28
Figure 2: Open Standards Reference Model [Culler 2011]	29

List of Tables

Table 1: Scoring Methodology	3
Table 2: Triage Table	5
Table 3: Open Systems Interconnection Model	27
Table 4: Examples of Underlying Technologies	30

Executive Summary

“The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.”

—Mark Weiser¹

Mark Weiser first coined the term *ubiquitous computing*, describing it as an “invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere.”² With advancements in miniaturization and in the economies of scale for systems-on-a-chip, Weiser’s vision is finally becoming a reality.

Weiser’s vision of the future also included the difficult challenge of securing the near-infinite amounts of data generated, processed, and stored by ubiquitous devices (or in today’s parlance, the “Internet of Things”). This increasing prevalence of new devices—and the extent to which Americans have come to rely on these devices in daily life—presents new challenges for the vulnerability coordination community. Can the Common Vulnerability Enumeration (CVE) methodology support this myriad of devices? Can the Common Vulnerability Scoring System (CVSS) provide effective and meaningful vulnerability information as increasingly complex and interrelated vulnerabilities surface?

The Department of Homeland Security’s United States Computer Emergency Readiness Team (US-CERT) “strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.”³ To carry out its mission, US-CERT must be proactive, focusing on future threats and vulnerabilities amid fear and uncertainty that often result from highly publicized cybersecurity attacks.

To support the US-CERT mission of proactivity, the CERT Coordination Center (CERT/CC) located at Carnegie Mellon University’s Software Engineering Institute was tasked with studying emerging systemic vulnerabilities, defined as exposures or weaknesses in a system that arise due to complex or unexpected interactions between subcomponents. The CERT/CC researched the emerging technology trends through 2025 to assess the technology domains that will become successful and transformative, as well as the potential cybersecurity impact of each domain. This report is intended to provide a brief background of each emerging technology domain along with a discussion of potential vulnerabilities and the risks of compromise or failure within each domain.

¹ <http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>

² <http://www.ubiq.com/hypertext/weiser/UbiHome.html>

³ <https://www.us-cert.gov>

This report also identifies the domains that should be prioritized for further study based on a number of factors. Five domains must be considered high-priority for outreach and analysis in 2016:

1. Networked Telematics
2. Smart Medical Devices
3. Autonomous Machines
4. Autonomous Vehicles
5. Commercial UAVs

This list does not imply that each domain will require detailed analysis. Every domain is nuanced, and some domains may require further study earlier in the technology development lifecycle of the domain than others. Approaches to improving security should be adjusted depending on the specific nature of each domain. In some cases, outreach is the best approach for improving the security of a technology; in other cases, technical vulnerability discovery may be the best way to provide better information to the government and public. This report includes a specific approach recommended by the CERT/CC for improving security in each domain.

This report will be updated every two years to include new domains, reassess the cybersecurity impact of each domain, and adjust the adoption timeline as needed.

Abstract

In today's increasingly interconnected world, the information security community must be prepared to address emerging vulnerabilities that may arise from new technology domains. Understanding trends and emerging technologies can help information security professionals, leaders of organizations, and others interested in information security to anticipate and prepare for such vulnerabilities. This report, originally prepared in 2015 for the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT), provides a snapshot in time of the current understanding of future technologies. This report will be updated every two years to include new estimates of adoption timelines, new technologies, and adjustments to the potential security impact of each domain. This report will also help US-CERT to make an informed decision about the best areas to focus resources for identifying new vulnerabilities, promoting good security practices, and increasing understanding of systemic vulnerability risk.

1 Introduction

As the world becomes increasingly interconnected through technology, information security vulnerabilities emerge from the deepening complexity. Unexpected interactions between hardware and software subcomponents can magnify the impact of a vulnerability. As technology continues its shift away from the PC-centric environment of the past to a cloud-based, perpetually connected world, it exposes sensitive systems and networks in ways that were never imagined.

The information security community must be prepared to address emerging systemic vulnerabilities—exposures or weaknesses in a system that are introduced due to complex or unexpected interactions between subcomponents. To help identify these vulnerabilities, the CERT Coordination Center (CERT/CC) located at Carnegie Mellon University’s Software Engineering Institute developed this report, which breaks down the major technology trends expected over the next 10 years. This report provides the background for further analysis work by the CERT/CC and will aid the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) in its work towards vulnerability triage, outreach, and analysis.

The goal of this report is to provide a snapshot in time of the current understanding of future technologies. This report will be updated every two years to include new estimates of adoption timelines, new technologies, and adjustments to the potential security impact of each domain. This report will also enable US-CERT to make an informed decision about areas where it should focus resources to identify new vulnerabilities, promote good security practices, and increase understanding of systemic vulnerability risk.

Report Format

This report presents information on 10 emerging domains⁴ and aims to provide the reader with

- an understanding of the major emerging technology domains
- the expected timeline for major worldwide adoption
- ways the domain may affect cybersecurity
- supporting standards and underlying technologies used by these domains
- likelihood of the domain becoming a success
- examples of exploitation in the domain or similar domains

The format of this report allows readers to quickly jump to a section and familiarize themselves with a domain. Each domain section contains the following subsections:

1. **Introduction** serves as a background on the application domain.
2. **Recommendation** includes the CERT/CC’s recommendation for US-CERT on addressing this domain.
3. **Time Frame** addresses the time and likelihood in which broad adoption is likely.

⁴ In this report, the term *domain* is used to describe a particular field of technology.

4. **Risks** provides a discussion of the potential impact of security vulnerabilities in the domain.
5. **Triage Table** describes the measures upon which the CERT/CC based its recommendations and how each domain was triaged for importance.
6. **Exploitation Examples** details concepts or existing research demonstrating exploits of this domain.

2 Methodology

A measured approach to analysis is required when undertaking the difficult task of reviewing all new and emerging technology domains, their likelihood of success, and any potential vulnerabilities. The CERT/CC used Gartner's long-term assessment of emerging technologies as a filter to form the initial list of domains [Burton and Walker 2015]. Gartner subscribers can access a list of "hype cycles" that describe each technology, its current maturity in the market, and when Gartner believes it will reach mainstream adoption in its industry [Fenn 2013]. This list tracks over 2,000 different technologies from inception to full adoption. From this list, the CERT/CC team identified domains likely to have an impact on global information security. Domains that were not included were either already widely deployed (e.g., mobile, cloud computing, supervisory control and data acquisition [SCADA]) or simply not applicable. For the 2016 report, the team triaged each identified domain according to the safety, privacy, financial, and operational impact (Table 1) that a cybersecurity incident could cause; the team used an approach adapted from ISO 26262 and the SAE paper *Threat Analysis and Risk Assessment in Automotive Cyber Security* (Table 2). If the impact score reached a total of four or higher (reflecting either serious risk in one or two domains, or low in all four), was <5-10 years away from adoption, and breaches a trust boundary, the domain was included in the analysis. The team then assessed each domain individually to determine its likelihood of success, potential impact if compromised, exploitation examples, and adoption timeline.

Table 1: Scoring Methodology

Class	Safety-Related Severity	Class	Financial-Related Severity
S0	No Injuries	S0	No financial loss
S1	Light or moderate injuries	S1	Low-level loss (~\$10)
S2	Severe and life-threatening injuries (survival probable) <i>Light or moderate injuries for multiple people</i>	S2	Moderate loss (~\$100) <i>Low losses for multiple people</i>
S3	Life threatening (survival uncertain) or fatal injuries <i>Severe injuries for multiple people</i>	S3	Heavy loss (~\$1,000) <i>Moderate losses for multiple people</i>
S4	Life threatening or fatal injuries for multiple people	S4	Heavy losses for multiple people

Class	Privacy-Related Severity	Class	Operational-Related Severity
S0	No unauthorized access to data	S0	No impact on operational performance
S1	Anonymous data only	S1	Impact not discernible to user
S2	Identification (personally identifiable information) of person or technology <i>Anonymous data for multiple people</i>	S2	User aware of performance degradation <i>Indiscernible impacts for multiple users</i>
S3	Tracking of individual or technology <i>Identification of multiple people or technologies</i>	S3	Significant impact on performance <i>Noticeable impact for multiple users</i>

S4	Tracking of multiple people or technologies
----	---

S4	Significant impact for multiple users
----	---------------------------------------

Table 2: Triage Table

Gartner's 2015 List of New Technology	Trust Boundary Breached? (Y/N)	Consumer/Enterprise? (C/E/Both)	Predicted Adoption Timeline	Safety	Privacy	Financial	Operational	Include?
Smart Dust	Y	E	10+	2	2	0	3	N
Virtual Personal Assistants	N	B	5-10	0	2	0	1	N
Digital Security	Y	B	5-10	0	0	0	3	N
People-Literate Technology	Y	B	5-10	0	1	1	1	N
Bioacoustic Sensing	N	B	10+	1	0	0	1	N
Quantum Computing	Y	E	10+	0	4	4	0	N
Brain-Computer Interface	Y	B	10+	2	2	0	0	N
Human Augmentation	Y	B	10+	4	2	0	1	N
Volumetric Displays	N	B	10+	0	0	0	0	N
3D Bioprinting Systems for Organ Transplant	N	E	5-10	4	0	0	0	N
Smart Robots	Y	B	5-10	4	3	1	4	Yes
Affective Computing	Y	C	5-10	0	2	0	0	N
Connected Home	Y	C	5-10	2	3	0	3	Yes
Biochips	N	C	5-10	0	4	0	0	N
Citizen Data Science	N	E	2-5	0	4	2	0	N
Neurobusiness	Y	B	10+	1	1	1	1	N
Software-Defined Security	Y	B	5-10	0	1	1	1	N
Digital Dexterity	N	E	5-10	0	0	0	0	N

Gartner's 2015 List of New Technology	Trust Boundary Breached? (Y/N)	Consumer/Enterprise? (C/E/Both)	Predicted Adoption Timeline	Safety	Privacy	Financial	Operational	Include?
Micro Data Centers	N	B	5-10	0	2	2	2	N
Smart Advisors	N	B	5-10	0	3	1	0	N
Advanced Analytics With Self-Service Delivery	N	B	2-5	0	2	1	1	N
Autonomous Vehicles	Y	B	5-10	4	2	0	3	Yes
Internet of Things	Y	B	5-10	3	2	0	2	Yes
Speech-to-Speech Translation	N	B	2-5	0	0	0	0	N
Machine Learning	N	B	2-5	0	0	0	2	No
Wearables	Y	B	5-10	0	2	0	0	No
Cryptocurrencies	N	B	5-10	0	1	3	0	N
Consumer 3D Printing	Y	B	5-10	2	2	0	1	Yes
Natural-Language Question Answering	Y	B	5-10	0	2	0	0	N
Hybrid Cloud Computing	Y	E	2-5	0	0	0	3	No
Augmented Reality	Y	B	5-10	3	2	0	2	Yes
Cryptocurrency Exchange	N	B	2-5	2	2	0	1	N
Autonomous Field Vehicles	Y	E	2-5	4	0	0	3	Yes
Virtual Reality	Y	B	5-10	1	2	0	0	N
Gesture Control	N	B	2-5	0	0	0	0	N
Enterprise 3D Printing	Y	E	2-5	2	0	0	4	Yes

Gartner's 2015 List of New Technology	Trust Boundary Breached? (Y/N)	Consumer/Enterprise? (C/E/Both)	Predicted Adoption Timeline	Safety	Privacy	Financial	Operational	Include?
Networked Telematics	Y	B		4	4	0	4	Yes
Smart Medical Devices	Y	E		4	4	0	4	Yes
Commercial UAVs	Y	E	2-5	4	0	0	4	Yes

3 Augmented Reality

3.1 Introduction

Augmented Reality (AR) uses technology to add context to a user's surrounding environment. Using real-time imagery and other sensor-provided input, an AR system aims to enhance or otherwise alter how people perceive physical reality.

Many examples of AR technology focus on rendering additional imagery or graphical cues on top of the user's line of sight. For example, some flight navigation systems are able to overlay recommended flight paths and visual indicators for runways, buildings, and other hazards onto the aircraft's forward-facing video feed.

While most uses of AR involve overlaying images onto video, some AR systems project images onto the surrounding physical environment. Non-invasive vein imaging devices, for example, can assist medical professionals by projecting an outline of the underlying veins directly onto a patient's skin [Miyake 2006].

3.2 Recommendation

The CERT/CC recommends further research of this domain in 2016 due to the growth of AR systems in military, medical, and infrastructure applications. The broad scope of these sectors suggests that the Department of Defense, the Department of Homeland Security, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the Food and Drug Administration (FDA), and the Federal Aviation Administration (FAA) will all take part in championing security efforts in this field.

3.3 Time Frame

Consumer and business applications of AR technology are already in use. The combined market for virtual and augmented reality technology could grow to \$150 billion in the next five years, with AR accounting for the vast majority (80%) of that market [Merel 2015].

3.4 Risks

Although some uses of AR do not pose a direct threat to human safety, some AR systems are relied upon as a primary source for mission-critical situational information. For example, a navigator using a navigation system may rely heavily upon the accuracy of the system's output to safely pilot a vehicle. Similarly, medical professionals must be able to trust the output of AR systems when using them to perform medical procedures. The criticality of such systems makes any compromise a potentially high-risk event to victims.

3.5 Exploitation Examples

In 2013, a researcher was able to uncover a vulnerability in Google Glass, a wearable device that provides AR features. The vulnerability essentially allowed researchers to coerce the device into connecting to attacker-controlled wireless access points after taking pictures of malicious quick

response (QR) codes. Successful exploitation of such a vulnerability could compromise the confidentiality and integrity of the device's network communications [Rogers 2013].

4 Connected Home

4.1 Introduction

The connected home represents the increasing automation of home devices, appliances, and computers that integrate with a centralized service for consumer use and control. The devices are diverse, from sensors (temperature, motion, movement, humidity) to controllers (smart thermostats, refrigerators, light bulbs), and are able to interact with the environment and each other. Online services such as If This Then That (IFTTT) and ThingSpeak provide a common platform to trigger actions to environmental stimuli on certain devices. For example, consumers can have their smartphone inform their house that they are close to home, turn on the lights, set the temperature, and disable the security alarms. In the 2014 report, this domain was called “Home Area Network” and “Smart Appliances.”

4.2 Recommendation

The CERT/CC recommends continuing focusing on improving the quality of home routers, the first line of defense for the connected home. For these consumer-level IoT devices, strive to maintain outreach capabilities to new vendors and encourage good security practices, especially performing security updates.

4.3 Time Frame

Gartner considers the connected home as being 5-10 years away from mainstream adoption. Business Insider estimates connected-home devices to reach 1.8 billion units in 2019 [Danova 2015].

4.4 Risks

The connected home is inherently vulnerable to attacks due to its reliance on a single defense—the home router. For most consumers, the security of the home network depends on the router's default security. Many home routers deployed today have outdated firmware and insecure configurations, and aren't supported by the vendor [Land 2015]. Other considerations include the security of the various connected devices.

4.5 Exploitation Examples

In 2014, the Belkin WeMo was shown to have a number of vulnerabilities associated with the platform [Allar 2014]. In 2015, researchers discovered vulnerabilities in a number of other IoT platforms, including applications such as garage door openers, smart sensors platforms, and voice-controlled virtual assistants [Smith 2015].

5 Enterprise 3D Printing (Additive Manufacturing)

5.1 Introduction

3D printing is an additive technique used to create three-dimensional objects by applying physical materials iteratively via an automated system. The term *printing* refers to the way an inkjet printer creates an image: by iteratively depositing ink over a sheet of paper. In 3D printing, materials such as plastics, fibers, metals, and even organic compounds can be used. The term *additive manufacturing* is becoming more commonplace.

3D printing has two general purposes in the enterprise: to generate prototypes in research, development, and product design, and to create actual products to sell to consumers. 3D printers constantly evolve to use more complex and durable materials, and their potential uses are increasing [Burns 2014].

5.2 Recommendation

The CERT/CC recommends further research of this domain in 2016. There is currently little evidence to suggest information security problems with 3D printing, but this situation may change as 3D printing enables consumers to print circuit boards and other electronic hardware.

5.3 Time Frame

3D printing has the potential to disrupt current manufacturing processes but will not be broadly adopted by home users in the near future. Adoption is expected to be small scale, with 3D printing being used primarily as a prototyping device for the next few years [Dignan 2014]. Today, a variety of 3D printers are already available, with rapid growth to 5.6 million units expected by 2019 (from 244,533 today) [Burns 2013; Franco 2014; Mearian 2015].

5.4 Risks

Additive manufacturing is not an area of explicit security concern. These devices contain Ethernet or Wi-Fi connectivity, a programmable logic controller, and various servomechanisms to control the heating units and distribution nozzles. While a security compromise of this device could result in damage to the device or the surrounding area (due to the heated material produced), these risks are not fundamentally different from those posed by existing industrial machinery.

One area that may prove to be a challenge to the information security community is the ability to custom-print keys (affecting physical security) or programmable logic boards or controllers. Cheap microcontroller/board development and open source designs allow for essentially unlimited production of sensors, micro PCs, and specialized equipment by a single individual. This democratization of hardware will have effects on the existing ecosystem of devices and systems that are difficult to predict.

5.5 Likelihood of Domain Success

Research and development and prototyping groups already make significant use of 3D printers and will continue to do so. In the near term, custom parts can be produced at various tooling companies that will become the first adopters of 3D printing. In the long term, the 3D printer may become just another tool like an auto-lathe or robotic assembly station.

5.6 Exploitation Examples

3D printers allow access to shapes and materials that were previously difficult to acquire in a covert fashion; 3D printers have been used to print restricted-use items such as handcuff keys and handgun parts [Greenberg 2012; Hsu 2013a; Hsu 2013b].

3D printers themselves can also be compromised directly, leading to other challenges [Xiao 2013; Titlow 2013]. As with a variety of automated manufacturing machines, the 3D printer must be configured with instructions that tell the printer what materials to deposit and where to place them. These instructions represent valuable intellectual property that can be stolen or even modified in place to produce “defective” items. In this way, 3D printing exposes all supply chain vulnerabilities and impacts, from manufacturing problems to impacts to customers when defects are not easily detected.

6 Networked Telematics

6.1 Introduction

Telematics refers to the electronics, communication, and display technology associated with vehicular dashboard systems. Telematics encompasses all functions of the vehicle electronics that are designed to be accessible to users. The dashboard, controls, and navigation system are parts of the telematics system. Many vehicle manufacturers have recently added cellular connectivity to their vehicles to provide richer, more interactive services to the consumer. Developers of smartphone operating systems have also begun to integrate their products more closely with telematics systems.

6.2 Recommendation

The CERT/CC recommends continued prioritization of this domain for outreach in 2016. The upcoming mass deployment of this domain will increase the risk of new vulnerabilities, especially those of a systemic nature. The emerging smartphone-telematics integration technologies (e.g., Apple CarPlay, Google Open Automotive Alliance, Blackberry QNX) are of particular concern.

6.3 Time Frame

Telematics systems, in varying levels of complexity, are deployed on practically every vehicle in the world. In the past, only a few vehicles had access to a cellular Internet connection, and only at 3G speeds. Some vehicles already have LTE connections, and many manufacturers plan to add them to future models [Cheng 2013, George 2014].

6.4 Risks

Telematics should be considered a high-risk domain for systemic vulnerabilities. A telematics system is very tightly integrated with other systems in a vehicle and provides a number of functions for the user. The recent additions of wireless connectivity such as Bluetooth, Wi-Fi, and LTE increase the risk of compromise. An Internet-connected vehicle is vulnerable to a wide range of attacks, both from determined attackers and from traditional threats such as malicious code and phishing.

6.5 Likelihood of Domain Success

This sector has a very high likelihood of success. Telematics systems are already deployed on most vehicles worldwide, and the major car manufacturers have announced that some 2015 and 2016 models will include LTE connections [Ziegler 2014, George 2014, Ziegler 2015].

6.6 Exploitation Examples

Academic researchers have looked deeply into the varied attack surfaces within vehicular systems, focusing on telematics in particular. This research has shown that it is possible to compromise a vehicle remotely via Bluetooth, malware-infected CDs, and through USB connection [Checkoway 2011]. Further research of a Jeep Cherokee's telematics system in 2015

resulted in the first recall of a vehicle due to cybersecurity issues [Greenberg 2015]. Researchers were able to remotely compromise recent Jeep and Fiat-Chrysler models using the same vulnerabilities in the shared telematics platform.

7 Smart Medical Devices

7.1 Introduction

A smart medical device is a biomechanical machine that interfaces with the human body in an inpatient or outpatient context. Recent advances in medical device development have moved the industry toward more connected devices, partly due to the benefits that the data from such devices can provide to central hospital systems. While caregivers see the trend toward smart medical devices as positive, security concerns increase as more devices are connected to the hospital network. Many of the devices in this field have little to no security, and the increased scrutiny required by the Food and Drug Administration (FDA) makes the patch cycle extremely long.

7.2 Recommendation

Due to the impact of smart medical devices on human lives, the CERT/CC recommends prioritizing outreach to this domain in 2016. The regulatory structure of this domain has shown that the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the FDA will be the primary champions of good security practices. In addition, the National Health Information Sharing and Analysis Center (NH-ISAC) has begun developing best practices to improve security of medical devices.

7.3 Time Frame

Smart medical device technology, part of the \$68 billion medical device market, is already deployed in many hospitals and clinics worldwide. Though smart medical devices are not yet ubiquitous, many of the new devices hospitals purchase are network-enabled and have some form of processing power and storage [Zhong 2012] .

7.4 Risks

As more devices are connected to hospital and clinic networks, patient data and information will be increasingly vulnerable. Even more concerning is the risk of remote compromise of a device directly connected to a patient. An attacker could theoretically increase or decrease dosages, send electrical signals to a patient, or disable vital sign monitoring.

7.5 Likelihood of Domain Success

This sector has a very high likelihood of success. Many manufacturers have released connected medical devices, and hospitals and clinics are purchasing more of these devices as they upgrade their equipment.

7.6 Exploitation Examples

The CERT/CC has received reports of vulnerabilities in network-enabled IV pumps, and other researchers have identified vulnerabilities in insulin pumps and pacemakers [Robertson 2013]. There have been no reports of targeted exploitation in the wild.

8 Autonomous Machines

8.1 Introduction

Smart robots, or autonomous machines, are independent, self-correcting, and learning machines. Unlike the robots of the past few decades, modern *smart robots* are increasingly user-friendly and integrated with the human worker. Traditional robots, including robots used on assembly lines, are able to complete rote tasks after considerable programming and configuration. Smart robots are able to learn a task through simple hand motions [Rethink Robotics 2014] or adjust transportation routes based on failures or in response to new data [Amazon Robotics 2016]. These autonomous systems are used to automate warehouse retrieval and storage [Symbiotic 2015, Amazon Robotics 2016], automate some part of a human task [Rethink Robotics 2014], mix and dose drugs [Intelligent Hospital Systems 2016], and transport items from one area to another in a hospital, warehouse, or other facility.

8.2 Recommendation

The CERT/CC recommends identifying major standards bodies and developing a list of companies for future outreach. This is a sector that is still developing and, as of now, has a low market share. As more of these smart robots become integrated with human workforces to automate tasks, they become a larger target of opportunity for an adversary.

8.3 Time Frame

Gartner considers smart robots as being 5-10 years away from mainstream adoption.

8.4 Impact

These devices could be compromised through networked back-end servers that provide some of the automation, or through the robot itself, which is networked and communicates across the Internet to the manufacturer for diagnostic information and software updates [Rethink Robotics 2014]. A compromised robot could cause destruction of property or death or injury of human workers. In some designs, control of these robots may be limited by hardware and safety programming. It may be technically impossible to cause a robot to harm a human due to these limitations, but due to the lack of detail presented in the research, the possibility of physical or economic harm cannot be ruled out.

8.5 Exploitation Examples

The CERT/CC is currently unaware of specific exploit examples as of the date of this publication.

9 Smart Sensors

9.1 Introduction

Smart sensors are one of the key technologies of ubiquitous computing, or the “Internet of Things” [Gubbi 2013]. Sensor technologies provide information about or control of a physical environment in response to certain stimuli. Two major types of sensors are being deployed by manufacturers: non-actuated and actuated sensors. Non-actuated sensors send information about the environment to a processing engine. Examples of non-actuated sensors include temperature sensors, vibration sensors, and soil moisture sensors. Actuated sensors send information about the environment but also receive commands or react to the environment in a particular way, usually by flipping an electronic switch or through mechanical manipulation. Examples of actuated sensors include wirelessly controllable smart lights, switches, and door locks. Both non-actuated and actuated sensors use wireless technologies to communicate. It should be noted that this domain is similar to SCADA, but it differs in that smart sensors use a greater number of standard network protocols and the Internet to facilitate communication. The differences between smart sensors and SCADA may decrease as SCADA gains more of the features that characterize this domain.

9.2 Recommendation

The CERT/CC recommends continued outreach for this domain in 2016 with a focus on commercial applications in particular.

9.3 Time Frame

The market for this domain is estimated between \$300 billion and \$7.1 trillion by 2020. In 2014, there were 16 billion wireless connected devices, and that number is expected to grow to 40 billion by 2020. The CERT/CC recommends engaging the standard bodies and companies involved in smart sensor creation before the devices reach broad-scale adoption [Press 2014].

9.4 Risks

Smart sensors contain wireless communication technology, limited processing power, and sometimes an actuator or electronic switch that allows the sensor to react to the environment. These devices can be used in a variety of ways, from smart thermostats that use motion detection and machine learning to change the temperature in a house, to smart lights equipped with special sensors that can communicate via wireless mesh networks, ad hoc communication architectures that allow devices to communicate whenever they come in range of other devices. This range of capabilities suggests that adversaries will be able to conduct attacks that affect our environment in ways that are difficult to predict. Privacy can be compromised if embedded cameras in smart lights are exploited, or adversaries may use their access to smart thermostats to assess whether or not a person is home. As these sensors are integrated more fully into daily life and provide more control to the user, it is likely that they will be increasingly considered a weak point into homes. Like many embedded devices with limited storage and processing, most of these sensors will

likely be difficult to upgrade; this difficulty will likely lead to an increase in older, unpatched vulnerabilities.

9.5 Likelihood of Domain Success

The smart sensor domain is likely to be successful. Sales of the Nest smart thermostat and intelligent smoke alarm products have increased, reaching over one million sales per year and rising [Yarrow 2014]. Smart lights are still nascent, but the massive energy savings are likely to make them ubiquitous in the commercial sector over the next several years [Digital Lumens 2013]. Belkin's consumer oriented WeMo line of smart plugs, lights, and devices provides remote control capability and some automation to everyday devices. During the 2015 holiday season, 50 million IoT devices were sold, and continued consumer and commercial interest in these devices suggests that growth will continue to be exponential (up to 11 trillion by 2025) [Gubbi 2013, Martin 2015, McKinsey 2015].

9.6 Exploitation Examples

In 2014, researchers found that the Belkin WeMo smart switch had several vulnerabilities that allowed an attacker to take complete control of the device, upload firmware, monitor other devices, and access the home network [Reuters 2014]. HP Enterprise Security Research reviewed 10 popular IoT devices and found a number of vulnerabilities, including 70% using unencrypted network services and 60% using unencrypted firmware updates [Hewlett-Packard 2015].

10 Commercial Unmanned Aerial Vehicles

10.1 Introduction

Commercial Unmanned Aerial Vehicles (UAVs), colloquially known as *drones*, are remotely operated and controlled by an operator with full control (via joystick) or controlled semi-autonomously (via map waypoints, for example). UAVs were initially developed for military applications to provide warfighters with remote strike capability without spending millions of dollars on manned aircraft. In recent years, the open source and commercial communities have developed UAVs for commercial applications. The increasing power of automation has allowed companies to build and test UAVs for traffic monitoring, surveillance, agriculture, filming, and shipping.

10.2 Recommendation

The CERT/CC recommends conducting background research and outreach to the FAA and other standards bodies in 2016. There is a clear potential for risk as drones become ubiquitous; being actively involved in the rulemaking will help to ensure the security and safety of these devices.

10.3 Time Frame

Commercial drones are still relatively nascent, but given the growth potential and interest from major corporations (Amazon, Google, Wal-Mart), drones will become more prevalent in the near future. There are also regulatory hurdles, as the FAA has only recently allowed low-flight UAVs to operate with prior approval and registration [FAA 2015].

10.4 Risks

Like any flying device, drones can be dangerous—they move quickly, and their movements are not restricted by controlled pathways such as roads. While the risks of bodily or property damage from a single drone are somewhat limited by the size and power of the device, fleets of networked, semi-autonomous drones present considerably more risk. A compromise of a drone fleet or even a widespread vulnerability could wreak havoc on shared airspace and on the people living below. If drones become more widely used, considerably more damage may be possible.

10.5 Likelihood of Domain Success

The market for commercial UAVs is expected to rise 19% (compounded annually) by 2020 [Business Insider 2015]. Consumer UAVs have increasingly gained capability due to inexpensive sensor technologies, GPS chips, and open source software. Commercially, Amazon and Google plan to develop and fly fleets of shipping drones for short-distance deliveries. In agriculture, drones are expected to be used for targeted “precision agriculture” to improve crop yields.

10.6 Exploitation Examples

Researchers were able to demonstrate live exploitation of Parrot AR drones using the built-in smartphone app, and they were able to exploit weaknesses in the Wi-Fi on the drone itself

[Culpan 2015]. In 2013, researcher Samy Kamkar developed SkyJack, which allowed a drone itself to autonomously seek and exploit other vulnerable drones [Kamkar 2013]. As of the time of this publication, there are no known examples of malicious exploitation of UAVs.

11 Vehicle Autonomy (Driverless Cars)

11.1 Introduction

Autonomous vehicles have the ability to move without direct commands from an operator. They can navigate to a destination using an autopilot-like capability, relying on onboard sensors, including GPS, cameras, lasers, and radar. These onboard sensors also enable autonomous vehicles to avoid potential obstacles.

The development of autonomous vehicles is touted as a revolutionary capability that will increase the safety and reliability of vehicles [IIHS 2010, Simonite 2013]. Autonomous vehicles can also help optimize fuel economy and manage traffic congestion using vehicular communication systems.

In an effort to classify and evaluate autonomous vehicle capability, the National Highway Traffic Safety Administration (NHTSA) has established five levels to clarify the continuum of technologies [NHTSA 2013]:

- **Level 0 (No Automation):** The driver is in complete and sole control of the vehicle (brake, steering, throttle, and motive power) at all times.
- **Level 1 (Function-Specific Automation):** One or more vehicle controls are automated. Examples include electronic stability control or pre-charged brakes, where the vehicle automatically assists with braking to enable the driver to regain control of the vehicle or stop faster than possible by acting alone.
- **Level 2 (Combined-Function Automation):** At least two primary control functions are automated and work in unison to relieve the driver of control of those functions. An example of combined-function automation is adaptive cruise control in combination with lane centering.
- **Level 3 (Limited Self-Driving Automation):** All safety-critical functions are automated, and the driver can choose to enable those automated functions under certain traffic or environmental conditions. Vehicles at this level of automation monitor for changes in conditions that require transition back to driver control. The driver is expected to be available for occasional control but with sufficiently comfortable transition time. The Google Self-Driving Car is an example of limited self-driving automation.
- **Level 4 (Full Self-Driving Automation):** The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip. Such a design relies on destination or navigation input from a human user, but a human driver is not expected to be available for control at any time during the trip. This type of vehicle can be occupied or unoccupied during a trip.

University research programs have studied various levels of automation over the years. These efforts progressed from basic research conducted in the 1980s and 1990s to the DARPA Grand Challenges in the mid-2000s. Autonomous vehicles recently developed by Google have logged hundreds of thousands miles in total on public roads without an automation-related incident [Tannert 2014]. Commercial vendors such as Audi, Toyota, Nissan, and General Motors are

currently investigating and demonstrating automation [Dassanayake 2014; Hsu 2013c; Turkus 2013; Krisher 2013].

11.2 Recommendation

The CERT/CC recommends continued research of the autonomous vehicle domain for outreach and analysis in 2016. This domain is being actively researched and tested by every major automobile manufacturer and by major technology companies such as Google, Apple, and Uber. Building an understanding and analysis capability in this field will allow for better outreach to manufacturers and researchers in the community. The massive safety benefits, transformation of lifestyle, and likely adoption mean that driverless cars will become an incredibly important technology. In addition, the potential for human harm and damage is very high, and the possible risks and vulnerabilities are not well understood.

11.3 Time Frame

Level 4 autonomous vehicles are not currently in production but are being tested by many major car manufacturers. In 2015, Tesla released an update for the Model S, giving drivers the ability to have Level 3 autonomy in their vehicle [Duffer 2015]. Planned 2017 model-year vehicles offer various degrees of autonomy: adaptive cruise control, lane control, and coordinated behaviors between cars. Manufacturers in domains that do not have the same restrictions as on-road driving are exploring more advanced levels of autonomy. Systems in these areas may be marketed or described as mobile robotic systems; examples include automated material handlers (forklifts), parking lot shuttles, and mining vehicles [Seegrid Corporation 2013; Vaughn 2014; Caterpillar 2013].

Level 1 capabilities such as electronic stability control are being mandated for new models; many of these capabilities are available now or will be available in the near term. Level 2 capabilities are about 5-10 years away. However, the building blocks for Level 2 capabilities are showing up in cars with Level 1 capabilities and in research and development projects such as the Super Cruise by General Motors [General Motors 2013]. At this time, Level 3 and 4 capabilities exist primarily in research environments and under strict human supervision.

11.4 Risks

Security concerns related to autonomous vehicles come predominantly from the potential for physical harm and damage. The digital disruption of autonomous vehicle systems has major implications for safety. For example, a software flaw affecting anti-lock brake systems in the Toyota Prius resulted in increased stopping distance [Toyota Motor Sales 2010].

Beyond the security concerns that are tied to basic flaws in implementation, there is the threat of active exploit. At DEFCON 2013, security researchers demonstrated attacks on vehicles [Greenberg 2013]. These attacks resulted in the compromise of the vehicle dashboard controls and displays, as well as the ability to cause a vehicle to brake or turn. At Black Hat 2015, researchers demonstrated remote access and exploitation of a passenger vehicle [Greenberg 2015]. Though these attacks were targeted at Level 1 and Level 0 capabilities, the implications for higher levels of autonomy are apparent. If low-level sensors and simplified systems are vulnerable to attack, compromise of Level 3 and 4 systems is inevitable.

11.5 Likelihood of Domain Success

Though fully autonomous vehicles are not ready for mainstream adoption, manufacturers are slowly rolling out functions that create the baseline of autonomous capability. In addition to technological challenges, policy and regulation are major barriers to large-scale deployment of autonomous vehicles. The automotive industry has many standards and regulations for vehicles. For broad adoption to occur, a consensus must be reached to ensure appropriate service levels for autonomy.

Individual states and legislative bodies are reviewing how autonomous vehicles can be governed by existing laws. States such as Florida, Nevada, and the District of Columbia have laws regarding the operation of autonomous vehicles but have differing opinions on liability and what constitutes an autonomous vehicle. The landscape of autonomous vehicles is so complex that the RAND Corporation created a guide to help inform policymakers about autonomous vehicles [Anderson 2014]. The report, *Autonomous Vehicle Technology: A Guide for Policymakers*, highlights the varying federal and state laws that may apply to vehicle autonomy as well as the liability issues surrounding autonomous vehicles.

11.6 Exploitation Examples

Researchers have identified information security problems in existing automotive systems that, for example, allow an attacker to modify vehicle displays and readouts or send arbitrary commands on the controller area network (CAN) bus [Koscher 2010; Miller 2013]. Another area of concern is GPS spoofing, but mitigating factors such as GPS modernization may limit this threat [Humphreys 2008; Nighswander 2012]. Finally, in 2015, the most severe car attack was demonstrated with the remote compromise of a passenger vehicle [Greenberg 2015]. So far, attacks have been limited, but they will likely increase in number, complexity, and damage as the technology becomes more connected.

12 Vehicular Communication Systems

12.1 Introduction

Vehicular communication systems combine wired and wireless technologies to enable intelligent transport systems for future cars, roads, and cities. Vehicular communication can be broken into two fields: Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) communication. V2V provides vehicles with the ability to communicate their speed, position, and other status information to nearby vehicles. V2I allows for vehicles to receive and send information to smart roads, tollbooths, and other infrastructure components.

12.2 Recommendation

With millions of vehicles expected to use this technology—and the potentially fatal consequences of failure—this domain is of high priority for further vulnerability analysis. Because vehicle manufacturers and standards bodies typically have a long development period for creating standards and regulatory requirements, the CERT/CC recommends continuing outreach and analysis efforts in 2016 to help influence this domain.

12.3 Time Frame

The U.S. Department of Transportation (DoT) Intelligent Transport System Office field-tested 3,000 vehicles equipped with V2V in a 2012 pilot program. Both the DoT and the NHTSA planned to support the advancement of this system in the consumer sector in 2014, and DoT officials have suggested that this technology may be mandatory for new vehicles starting in 2017 [NHTSA 2014; Nawaguna 2014]. The first V2V capable vehicle, the 2017 Cadillac CTS, will be on the road in 2016 [Bigelow 2015].

12.4 Risks

The DoT and NHTSA have stated that, in the initial rollout of the technology in vehicles and infrastructure, V2V and V2I will only communicate safety warnings to the driver, not control functionality. The 5.9Ghz spectrum is currently reserved by the Federal Communications Commission (FCC) for this technology, and that spectrum is shared with Wi-Fi devices. While the DoT and NHTSA insist that vehicular communication systems have many safeguards to protect privacy and automobiles, the simple act of providing an open communication path to a vehicle introduces risk. Recent vehicular automotive vulnerability research has demonstrated that the introduction of new technology into a vehicle can create behavior that the manufacturer did not intend [Miller 2013]. The future use of this technology as a control mechanism introduces even more risks, including those with fatal results.

12.5 Likelihood of Domain Success

This technology will be deployed in the Cadillac 2017 CTS [Bigelow 2015]. Manufacturers and regulators are working toward the development and deployment of this technology. Standards are

available for use by manufacturers, pilot tests have been completed, and a mandate for use may be in place by 2017 [NHTSA 2013].

12.6 Exploitation Examples

So far, there are no known examples of exploitation of vehicular communication systems. Research in related domains has revealed systemic vulnerabilities that allow attackers to access the underlying electromechanics of the vehicle to gain control or provide improper readings to the driver [Checkoway 2011; Koscher 2010; Miller 2013]. In some cases, the researchers were able to remotely compromise the vehicle.

13 Conclusion

In preparing this report, the CERT/CC analyzed emerging technologies that are expected to become mature before 2025. This analysis resulted in a list of 10 technology domains of cybersecurity interest. For each domain, the team developed a brief background, recommendations for research, an expected time frame of adoption, impacts of vulnerabilities, likelihood of success, and exploitation examples. This report provides an understanding of cybersecurity issues that may result as part of each domain's adoption in the future.

This report also identifies the domains that should be prioritized for further study based on a number of factors. The five domains that must be considered high-priority for outreach and analysis in 2016 are:

1. Networked Telematics
2. Smart Medical Devices
3. Autonomous Machines
4. Autonomous Vehicles
5. Commercial UAVs

Appendix A: Underlying Technologies

Emerging technologies tend to leverage existing technologies—rather than reinventing the wheel—to improve the likelihood of adoption. By examining some of the underlying technologies we can more accurately assess potential vulnerabilities. This section describes some of the general threats to these technologies and gives short descriptions of the protocols evaluated as part of this report. This list is by no means comprehensive and is intended to provide coverage of popular protocols that exist today.

With the rapid development and deployment of devices, established infrastructure communication methods are quickly declining. New devices are relying more on wireless communication instead of using traditional wired communication. This departure from wired systems allows for rapid deployment and minimal infrastructure costs. As this shift continues, there is movement from infrastructure wireless to mesh-based networking solutions even within wireless communications. This focus on wireless communications in emerging technologies is the motivation behind this section and our emphasis on wireless communication technology and protocols.

One way to describe communication interconnects is by describing the network by spatial scope. Some common examples describing spatial scope are

- Body Area Network (BAN)
- Personal Area Network (PAN)
- Local Area Network (LAN)
- Wide Area Network (WAN)

Each of these networks has multiple options for communications protocols to use, from Bluetooth for BANs and PANs, to Ethernet (IEEE 802.3) for LANs, to WiMAX and LTE for WANs.

Another way to view these networks is through the common Open Systems Interconnection (OSI) model. This seven-layer model describes progressively higher level functions (see Table 3).

Table 3: Open Systems Interconnection Model

OSI Model	Data unit	Layer	Function
Host Layers	Data	7. Application	Network Process
		6. Presentation	Data representation
		5. Session	Interhost Communication
	Segments	4. Transport	Reliable delivery of packets
Media Layers	Packet/Datagram	3. Network	Addressing, routing, and delivery of datagrams
	Bit/Frame	2. Data link	Reliable, direct point-to-point data connections
	Bit	1. Physical	Direct point-to-point data connections

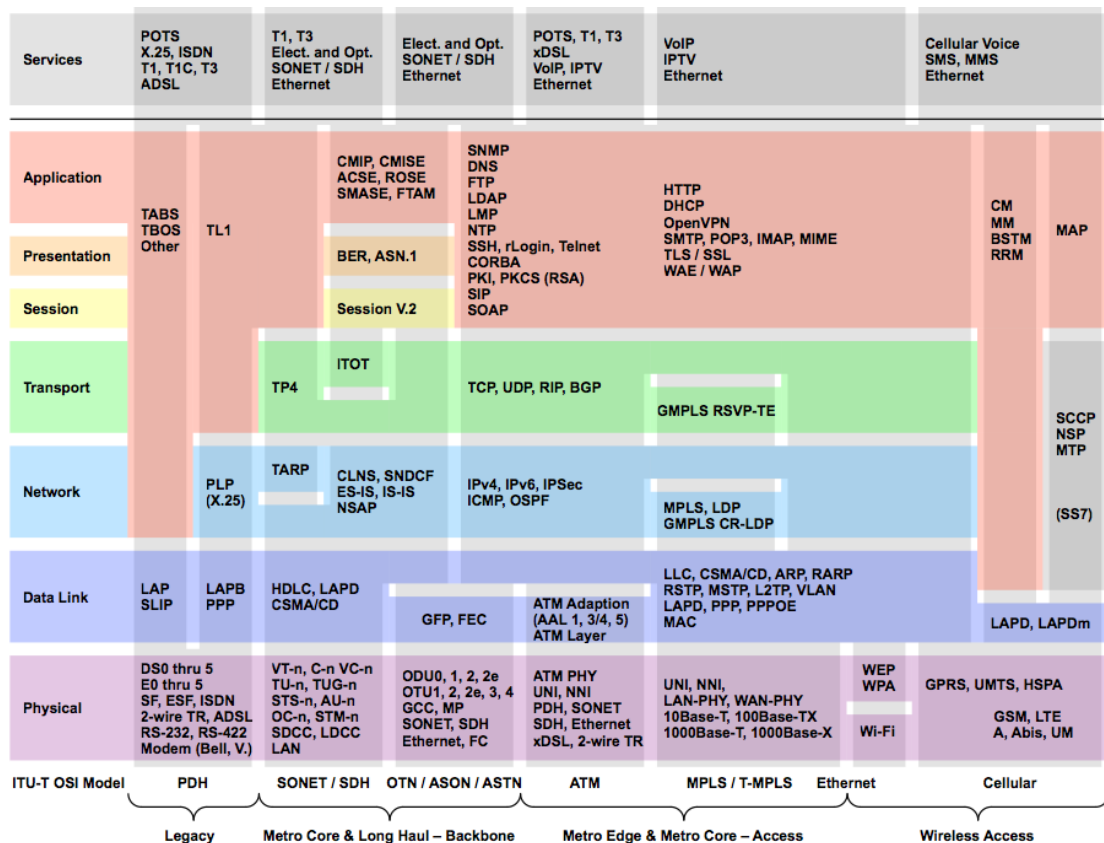


Figure 1: Communication Layers, Standards, and Technologies [Tele-Worx 2014]

As shown in Figure 1, protocols and implementations can exist at various layers and can even span layers. As wireless devices seek performance gains, new research has shown that blurring the lines of the traditional OSI model is beneficial though others are pushing back for standardization [Raisinghani 2004; van der Schaar 2005; Mehlman 2014]. The varying scope and touch points for each of these protocols can be indicative of vulnerable locations. Well-defined boundaries are not necessarily in place, and each of these protocols could be vulnerable to security issues related to implementing the interface.

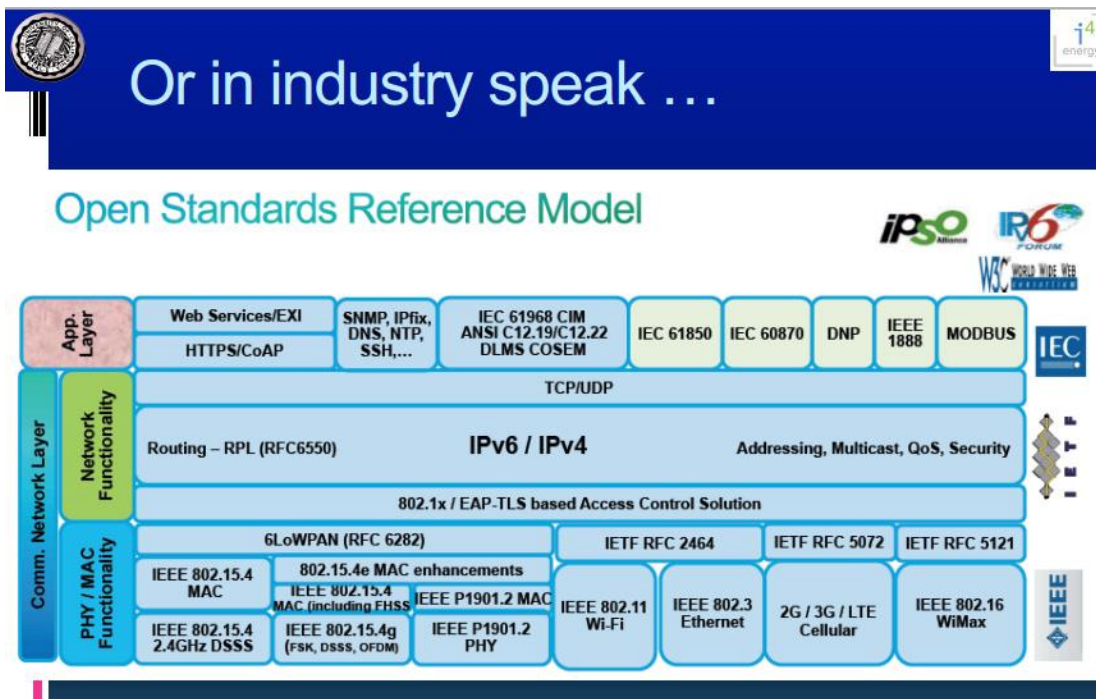


Figure 2: Open Standards Reference Model [Culler 2011]

Communication protocol stacks can have similar vulnerabilities given their position in the architecture. The lower layers are in direct communication with the hardware and can be vulnerable to different forms of hardware, firmware, and baseband attacks. In addition, high-performance networks usually rely on direct memory access (DMA) to achieve high throughput. DMA has the potential for memory exploitation given the trust it has given the architecture. In addition to the underlying attacks, each protocol may have unique vulnerabilities (e.g., IEEE 802.11's WEP standard was broken, and Bluetooth has default pairing code vulnerabilities).

Table 4: Examples of Underlying Technologies

Protocol	Type of Network	Spatial Category	Typical Applications	Other Notes
6LoWPAN (IPv6 over Low power Wireless Personal Area Networks)	Point-to-Point, Point-to-Multipoint/Star	PAN		
ANT	Mesh, Point-to-Point, Tree, Point-to-Multipoint/Star	PAN	Primarily fitness performance monitoring	
Bluetooth (IEEE 802.15.1)	Point-to-Point, Point-to-Multipoint/Star (>v4.0)	PAN	Phones, Tablets, Media Players, Watches, Headsets, Speakers, Input Devices, etc.	
Bluetooth Low Energy	Point-to-Point	PAN	See Bluetooth.	Simpler, non-backwards-compatible version of Bluetooth.
Cellular	Point-to-Point	WAN	Phones, Computers, Tablets, Smart Meters, Cars	
Dash7 / ISO-IEC 18000-7	Point-to-Point	WAN	Sensor Networks	
Ethernet (IEEE 802.3)	Point-to-Point	LAN	Computers	
Global Positioning System	Broadcast-only	Worldwide	Position, Velocity, Time	
IEEE 802.15.4 (Low Rate Personal Wireless Network - LW-PWAN)	Point-to-Point	Depends on implementation	Sensor Networks	
NFC	Point-to-Point	NFC	Mobile Payments, low bandwidth communication	
RFID	Point-to-Point	PAN	Access control, Tracking solutions	
Wireless Access in Vehicular Environments (WAVE) (IEEE 802.11p)	Point-to-Point	CAN	Vehicle based communication networks.	
Wi-Fi 33 (IEEE 802.11)	Point-to-Point, Point-to-Multipoint/Star	LAN	Phones, Computers	
ZigBee	Point-to-Point, Mesh	LAN	Sensor Networks	
Z-Wave	Point-to-Point, Mesh	LAN	Sensor Networks	

References/Bibliography

URLs are valid as of the publication date of this document.

[Allar 2014]

Allar, Jared. “Belkin Wemo Home Automation devices contain multiple vulnerabilities.” <https://www.kb.cert.org/vuls/id/656302> (February 18, 2014).

[Amazon Robotics 2016]

Amazon Robotics. <https://www.amazonrobotics.com/>

[Anderson 2014]

Anderson, James M.; Kalra, Nidhi; Stanley, Karlyn D.; Sorensen, Paul; Samaras, Constantine; & Oluwatola, Oluwatobi A. *Autonomous Vehicle Technology: A Guide for Policymakers*. http://www.rand.org/pubs/research_reports/RR443-1.html (2014).

[Bigelow 2015]

Bigelow, Pete. “Combine a self-driving car with V2V, and here’s what happens.” <http://www.autoblog.com/2015/12/12/autonomous-car-delphi-v2v-vehicle-ces/> (December 12, 2015).

[Burton and Walker 2015]

Burton, Betsy and Walker, Mike. *Hype Cycle for Emerging Technologies, 2015*. <https://www.gartner.com/doc/3100227/hype-cycle-emerging-technologies-> (July 27th, 2015)

[Burns 2014]

Burns, Matt. *The World’s First Carbon Fiber 3D Printer Is Now Available to Order*. <http://techcrunch.com/2014/02/18/the-worlds-first-carbon-fiber-3d-printer-is-now-available-to-order> (February 18, 2014).

[Burns 2013]

Burns, Matt. *Enterprise-Class 3D Printers to Drop Under \$2,000 by 2016, Says Report*. <http://techcrunch.com/2013/03/29/enterprise-class-3d-printers-to-drop-under-2000-by-2016-says-report/> (March 29, 2013).

[Business Insider 2015]

Business Insider. “The Drones Report: Market forecasts, regulatory barriers, top vendors, and leading commercial applications.” <http://www.businessinsider.com/uav-or-commercial-drone-market-forecast-2015-2> (May 27, 2015).

[Caterpillar 2013]

Caterpillar. *Caterpillar and Fortescue: Moving Forward with Commercial Installation of Autonomous Trucks*. <http://www.mining.com/web/caterpillar-and-fortescue-moving-forward-with-commercial-installation-of-autonomous-trucks/> (2013).

[Checkoway 2011]

Checkoway, Stephen; McCoy, Damon; Kantor, Brian; Anderson, Danny; Shacham, Hovav; Savage, Stefan. *Comprehensive Experimental Analyses of Automotive Attack Surfaces*. <http://www.autosec.org/pubs/cars-usenixsec2011.pdf> (2011).

[Cheng 2013]

Cheng, Roger. *AT&T, General Motors to Sell 4G LTE-Connected Cars Next Year*. <http://www.cnet.com/news/at-t-general-motors-to-sell-4g-lte-connected-cars-next-year/> 2013 (February 24, 2013).

[Culler 2011]

Culler, David E. "The Internet of Every Thing – steps toward sustainability." Keynote, China Conference on Wireless Sensor Network. September 26, 2011. www.cs.berkeley.edu/~culler/talks/Culler-CWSN.pptx

[Culpan 2015]

Culpan, Daniel. "Watch this drone being live hacked." <http://www.wired.co.uk/news/archive/2015-08/19/drone-hack-defcon> (August 9, 2015).

[Danova 2015]

Danova, Tony. "THE CONNECTED-HOME REPORT: Forecasts and growth trends for one of the top 'Internet of Things' markets." <http://www.businessinsider.com/connected-home-forecasts-and-growth-2014-9> (March 16, 2015).

[Dassanayake 2014]

Dassanayake, Dion. *CES 2014: Audi Unveils Prototype Autonomous Car with 'Auto-Pilot' System*. <http://www.express.co.uk/news/science-technology/452562/CES-2014-Audi-unveils-prototype-autonomous-car-with-auto-pilot-system> (January 7, 2014).

[Digital Lumens 2013]

Digital Lumens. LightRules 2.5 Product Specifications. http://www.digitallumens.si/images/LightRules_Specifications.pdf (2013).

[Dignan 2014]

Dignan, Larry. *3D Printing: Mainstream Adoption in 2014?* <http://www.zdnet.com/3d-printing-mainstream-adoption-in-2014-7000024701> (January 2, 2014).

[Dillow 2015]

Dillow, Clay. "Why 2015 is the year agriculture drones take off." <http://fortune.com/2015/05/18/drone-agriculture/> (May 18, 2015).

[Duffer 2015]

Duffer, Robert. "Tesla autopilot turns driver on to not driving." <http://www.chicagotribune.com/classified/automotive/sc-tesla-models-autopilot-1210-20151207-story.html> (December 8, 2015).

[FAA 2015]

Federal Aviation Administration. Unmanned Aircraft Systems (UAS) Frequently Asked Questions. <https://www.faa.gov/uas/faq/> (December 22, 2015).

[Fenn 2013]

Fenn, Jackie & Raskino, Mark. *Understanding Gartner's Hype Cycles*. <http://www.gartner.com/document/code/251964> (July 2, 2013).

[Franco 2014]

Franco, Michael. *Skyforge, a Vending Machine for Your 3D-Printed Dreams*. http://news.cnet.com/8301-11386_3-57618264-76/skyforge-a-vending-machine-for-your-3d-printed-dreams (February 4, 2014).

[General Motors 2013]

General Motors. *'Super Cruise' Takes on Real-World Traffic Scenarios*. <http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2013/Apr/0429-cadillac-super-cruise.html> (April 29, 2013).

[George 2014]

George, Alexander. *New In-Car LTE Finally Brings Netflix Binges to Your Commute*. <http://www.wired.com/2014/03/audi-cadillac-4g-lte/> (March 17, 2014).

[Greenberg 2015]

Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway—With Me in It" <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> (July 21, 2015).

[Greenberg 2013]

Greenberg, Andy. *Hackers Reveal Nasty New Car Attacks—with Me Behind the Wheel*. <http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/> (July 24, 2013).

[Greenberg 2012]

Greenberg, Andy. *Hacker Opens High Security Handcuffs with 3D-Printed and Laser-Cut Keys*. <http://www.forbes.com/sites/andygreenberg/2012/07/16/hacker-opens-high-security-handcuffs-with-3d-printed-and-laser-cut-keys> (July 16, 2012).

[Gubbi 2013]

Gubbi, Jayavardhana; Buyya, Rajkumar; Marusic, Slaven; & Palaniswami, Marimuthu. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." *Future Generation Computer Systems* 29, 7 (September 2013): 1645-1660.

[Hewlett-Packard 2015]

Hewlett-Packard. Internet of things research study. <http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en> (2015).

[Hsu 2013a]

Hsu, Jeremy. *3-D Printed Gun's First Shot Has Big Implications*. <http://spectrum.ieee.org/tech-talk/consumer-electronics/gadgets/3dprinted-guns-firing-shot-has-big-implications> (May 8, 2013).

[Hsu 2013b]

Hsu, Jeremy. *First 3-D-Printed Metal Gun Shows Tech Maturity*. <http://spectrum.ieee.org/tech-talk/robotics/industrial-robots/first-3dprinted-metal-gun-shows-tech-maturity> (Nov 7, 2013).

[Hsu 2013c]

Hsu, Tiffany. *CES 2013: Lexus Driverless Car: 'Technology Alone Is Not the Answer.'* <http://articles.latimes.com/2013/jan/07/autos/la-fi-tn-ces-hy-lexus-driverless-car-20130107> (January 7, 2013).

[Humphreys 2008]

Humphreys, Todd E.; Ledvina, Brent M.; Psiaki, Mark L.; O'Hanlon, Brady W.; & Kintner, Jr., Paul M. "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," 2314-2325. *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008)*. Savannah, Georgia, September 16-19, 2008. Institute of Navigation, 2008.

[IIHS 2010]

Insurance Institute for Highway Safety (IIHS). "New Estimates of Benefits of Crash Avoidance Features on Passenger Vehicles." *Status Report*, 45, 5 (May 20, 2010). <http://www.iihs.org/iihs/sr/statusreport/article/45/5/2>

[Intelligent Hospital Systems 2016]

Intelligent Hospital Systems. <http://www.intellighenthospitals.com/IHS/solutions.php> (January 10, 2016).

[Kamkar 2013]

Kamkar, Samy. *Applied Hacking*. <http://samy.pl/skyjack/> (December 2, 2013).

[Koscher 2010]

Koscher, Karl et al. "Experimental Security Analysis of a Modern Automobile," 447-462. *IEEE Symposium on Security and Privacy*. Oakland, California, May 16-19, 2010. IEEE, 2010. <http://www.autosec.org/pubs/cars-oakland2010.pdf>

[Krisher 2013]

Krisher, Tom. *GM to Offer Nearly Self-Driving Car by 2020*. <http://www.usatoday.com/story/money/cars/2013/08/30/gm-general-motors-self-driving-autonomous-car/2725091/> (August 30, 2013).

[Land 2015]

Land, Joel. Belkin N600 DB Wireless Dual Band N+ router contains multiple vulnerabilities. <https://www.kb.cert.org/vuls/id/201168> (August 31, 2015).

[Martin 2015]

Martin, Chuck. "Internet Of Things Holiday Sales: 50 Million Smart Objects." <http://www.mediapost.com/publications/article/264394/internet-of-things-holiday-sales-50-million-smart.html> (December 10, 2015).

[McKinsey 2015]

McKinsey. *THE INTERNET OF THINGS:MAPPING THE VALUE BEYOND THE HYPE*. <http://www.mckinsey.com/~media/McKinsey/Business%20Functions/Business%20Technology/>

Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Full_report.ashx (June 2015).

[Mearian 2015]

Mearian, Lucas. Low-cost 3D printers driving massive growth.

<http://www.computerworld.com/article/2987607/3d-printing/low-cost-3d-printers-driving-massive-growth.html> (September 30, 2015).

[Mehlman 2014]

Mehlman, Jeffrey. *Cross-Layer Design: A Case for Standardization*.

http://www.tc.ait.ac.th/faculty/teerapat/AT77.9019_Cross-Layer_Design_for_Wireless_Networks/Reading%20Assignments/Cross-layer%20Design_A_case_standardization.pdf (2014).

[Merel 2015]

Merel, Tim. Augmented And Virtual Reality To Hit \$150 Billion, Disrupting Mobile By 2020.

<http://techcrunch.com/2015/04/06/augmented-and-virtual-reality-to-hit-150-billion-by-2020/> (April 6, 2015).

[Miller 2013]

Miller, Charlie & Valasek, Chris. *Adventures in Automotive Networks and Control Units*.

http://illmatics.com/car_hacking.pdf (2013).

[Miyake 2006]

Miyake, Roberto Kasuo et al. Vein Imaging: A New Method of Near Infrared Imaging, Where a Processed Image Is Projected onto the Skin for the Enhancement of Vein Treatment.

<https://www.christiemed.com/Documents/clinical%20studies/A-New-Method-of-Near-Infrared.pdf> (August 2006).

[Mountz 2012]

Mountz, Mick. Kiva the Disruptor. <https://hbr.org/2012/12/kiva-the-disrupter> (December 12, 2012).

[Nawaguna 2014]

Nawaguna, Elvina. *Update 2-U.S. May Mandate 'Talking' Cars by Early 2017*.

<http://www.reuters.com/article/2014/02/03/autos-technology-rules-idUSL2N0L814120140203> (February 3, 2014).

[NHTSA 2013]

National Highway Traffic Safety Administration (NHTSA). *U.S. Department of Transportation Releases Policy on Automated Vehicle Development*.

<http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development> (May 30, 2013).

[Nighswander 2012]

Nighswander, Tyler et al. "GPS Software Attacks," 450-461. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. Raleigh, North Carolina, October 16-18, 2012. ACM, 2012.

[Press 2014]

Press, Gil. *Internet of Things By The Numbers: Market Estimates And Forecasts*.
<http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/> (August 22, 2014).

[Raisinghani 2004]

Raisinghani, Vijay T. & Iyer, Sridhar. "Cross-Layer Design Optimizations in Wireless Protocol Stacks." *Computer Communications* 27, 8 (May 2004): 720-724.

[Rethink Robotics 2014]

Rethink Robotics. "Baxter Helps The Rodon Group Stay 'Cheaper Than China.'" http://www-staging.rethinkrobotics.com/wp-content/uploads/2014/08/Rodon_Spotlight_final.9.13.pdf (September 9, 2014).

[Reuters 2014]

Reuters. *IOActive Lights Up Vulnerabilities for Over Half a Million Belkin WeMo Users*.
<http://www.reuters.com/article/2014/02/18/idUSnMKWhLTXta+1dc+MKW20140218> (February 18, 2014).

[Robertson 2013]

Robertson, Jordan. *Medical Device Hackers Find Government Ally to Pressure Industry*.
<http://www.bloomberg.com/news/2013-07-22/medical-device-hackers-find-government-ally-to-pressure-industry.html> (July 23, 2013).

[Rogers 2013]

Rogers, Marc. "Hacking the Internet of Things for Good."
<https://blog.lookout.com/blog/2013/07/17/hacking-the-internet-of-things-for-good/> (July 17, 2013).

[Seegrid Corporation 2013]

Seegrid Corporation. *Flexible Automated Guided Vehicles Anticipate Huge Growth in Europe 2014*. <https://www.prlog.org/12260112-seegrid-flexible-automated-guided-vehicles-anticipate-huge-growth-in-europe-2014.html> (December 24, 2013).

[Simonite 2013]

Simonite, Tom. *Data Shows Google's Robot Cars Are Smoother, Safer Drivers Than You or I*.
<http://www.technologyreview.com/news/520746/data-shows-googles-robot-cars-are-smoother-safer-drivers-than-you-or-i/> (October 25, 2013).

[Smith 2015]

Smith, Ms. "Attackers can stalk or rob you by exploiting IoT device security and privacy flaws."
<http://www.networkworld.com/article/2906723/microsoft-subnet/attackers-can-stalk-or-rob-you-by-exploiting-iot-device-security-and-privacy-flaws.html> (April 18, 2015).

[Swisslog 2015]

Swisslog. RoboCourier® Autonomous Mobile Robot.
<http://swisslog.com/en/Products/HCS/Automated-Material-Transport/RoboCourier-Autonomous-Mobile-Robot> (2015).

[Symbiotic 2015]

Symbiotic. <http://www.symbiotic.com/solutions/> (2015).

[Tannert 2014]

Tannert, Chuck. *Self-Driving Cars: Inside the Road Revolution*.

<http://www.fastcompany.com/3022489/innovation-agents/self-driving-cars-let-go-of-the-wheel> (January 8, 2014).

[Tele-Worx 2014]

Tele-Worx. *Network Interface and Protocol Expertise—from the Application to the Physical Media*. http://www.tele-worx.com/TELE-WORX/Interface_and_Protocol_Expertise.html (2014).

[Titlow 2013]

Titlow, John Paul. *How Hackers Can Infiltrate a 3-D Printer*.

<http://www.fastcolabs.com/3013165/inside-3-d-printings-weird-illicit-and-dangerous-fringe> (August 6, 2013).

[Toyota Motor Sales 2010]

Toyota Motor Sales. *Toyota Announces Voluntary Recall on 2010 Model-Year Prius and 2010 Lexus HS 250h Vehicles to Update ABS Software*.

http://www.lexus.com/recall/pdf/HS_Recall_Press_Release.pdf (February 8, 2010).

[Turkus 2013]

Turkus, Brandon. *Nissan Promising Autonomous Car Production by 2020*.

<http://www.autoblog.com/2013/08/27/nissan-promising-autonomous-car-production-by-2020/> (August 27, 2013).

[Vaughn 2014]

Vaughn, Mark. *This Could Be Your First Autonomous Vehicle*. <http://autoweek.com/article/car-news/could-be-your-first-autonomous-vehicle> (January 8, 2014).

[van der Schaar 2005]

van der Schaar, M. & Sai, Shankar N. “Cross-Layer Wireless Multimedia Transmission: Challenges, Principles, and New Paradigms.” *Wireless Communications, IEEE 12*, 4 (August 2005): 50-58.

[Xiao 2013]

Xiao, Claud. *Security Attack to 3D Printing*. XCon2013 XFocus Security Conference. Beijing, China, August 22-23, 2013. <http://www.claudxiao.net/Attack3DPrinting-Claud-en.pdf>

[Yarow 2014]

Yarow, Jay. *Nest, Google’s New Thermostat Company, Is Generating A Stunning \$300 Million in Annual Revenue*. <http://www.businessinsider.com/nest-revenue-2014-1> (January 14, 2014).

[Zhong 2012]

Zhong, Han. *Primer: The Medical Device Industry*.

http://americanactionforum.org/sites/default/files/OHC_MedDevIndPrimer.pdf (June 2012).

[Ziegler 2014]

Ziegler, Chris. "Cars are the new smartphones: Chevrolet adding LTE and app store to 2015 models." <http://www.theverge.com/2014/1/5/5276536/cars-are-the-new-smartphones-chevrolet-adding-lte-and-app-store-to-2015-models> (January 5, 2014).

[Ziegler 2015]

Ziegler, Chris. "Ford will add LTE to way more cars with new Sync Connect service." <http://www.theverge.com/2015/11/17/9742532/ford-sync-connect-lte-2017-ford-escape> (November 17, 2015).

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE April 2016	3. REPORT TYPE AND DATES COVERED Final		
4. TITLE AND SUBTITLE 2016 Emerging Technology Domains Risk Survey		5. FUNDING NUMBERS FA8721-05-C-0003		
6. AUTHOR(S) Christopher King, Dan Klinedinst, Todd Lewellen, & Garret Wassermann				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2016-TR-003		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116		10. SPONSORING/MONITORING AGENCY REPORT NUMBER n/a		
11. SUPPLEMENTARY NOTES				
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS		12B DISTRIBUTION CODE		
13. ABSTRACT (MAXIMUM 200 WORDS) In today's increasingly interconnected world, the information security community must be prepared to address emerging vulnerabilities that may arise from new technology domains. Understanding trends and emerging technologies can help information security professionals, leaders of organizations, and others interested in information security to anticipate and prepare for such vulnerabilities. This report, originally prepared in 2015 for the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT), provides a snapshot in time of the current understanding of future technologies. This report will be updated every two years to include new estimates of adoption timelines, new technologies, and adjustments to the potential security impact of each domain. This report will also help US-CERT to make an informed decision about the best areas to focus resources for identifying new vulnerabilities, promoting good security practices, and increasing understanding of systemic vulnerability risk.				
14. SUBJECT TERMS emerging technology, vulnerabilities, autonomy, internet of things		15. NUMBER OF PAGES 48		
16. PRICE CODE				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102